Article

Not peer-reviewed version

healthMLsec: Machine Learning based Vulnerability Assessment in Health Systems: A Framework for Enhancing Cybersecurity and Patient Data

Omar Faruq Osama , Naresh Kshetri * , Mir Mehedi Rahman , Bishwo Prakash Pokharel

Posted Date: 27 February 2025

doi: 10.20944/preprints202502.2165.v1

Keywords: Cyber Attacks; Cybersecurity; Emerging Threats; Healthcare; Machine Learning; Patient Data; Vulnerability

Article

healthMLsec: Machine Learning based Vulnerability Assessment in Health Systems: A Framework for Enhancing Cybersecurity and Patient Data

Omar Faruq Osama [1,*], Mir Mehedi Rahman [2], Naresh Kshetri [3] and Bishwo Prakash Pokharel [4]

[1] Dept. of System Science & Ind. Eng., Binghamton Univ., SUNY
[2] Department of Cybersecurity, Rochester Institute of Technology
[3] School of Business and Technology, Emporia State University
[4] Sault College of Applied Arts and Technology
[*] Correspondence: oosama@binghamton.edu

Abstract: In the advancing digital realm of healthcare, cyberattacks present substantial hazards to patient data integrity, privacy, including whole system security. As healthcare organizations increasingly depend on correlated digital platforms, it is essential to detect and prioritize vulnerabilities inside these systems to protect sensitive patient information. This study presents a machine learning based framework aimed at evaluating and mitigating cybersecurity risks in healthcare systems. The framework uses machine learning techniques to investigate extensive amounts of systems along with network data, detecting patterns that may indicate possible security vulnerabilities. The methodology facilitates the effective allocation of resources by prioritizing vulnerabilities according to their severity and probability of exploitation, allowing health organizations to concentrate on the most significant risks. Additionally, the proposed approach persistently adjusts to emerging threats by assimilating fresh data, confirming that the vulnerability analysis stays relevant among increasing cyber threats. This proactive strategy improves patient data security, cybersecurity against vulnerability, and complies with regulatory standards, hence reinforcing confidence in digital health systems. The study highlights the capability of machine learning to enhance cybersecurity resilience in healthcare, providing a strong, scalable approach for vulnerability evaluation and remediation with conclusion as well as future scope of the study.

Keywords: Cyber Attacks; Cybersecurity; Emerging Threats; Healthcare; Machine Learning; Patient Data; Vulnerability

I. Introduction

Technological advancements have significantly enhanced the efficiency of the health care sector. The appropriate integration of information technology with healthcare organizations has facilitated convenient and cost-effective service access for relevant stakeholders. Systems, such as patient portals, Laboratory Information Systems, clinical decision support, electronic health records, and remote patient monitoring, have substantially improved service delivery and patient outcomes. These systems are interconnected with other systems for real-time information accessibility and assisting healthcare professionals in optimizing workflow along with facilitating appropriate decision-making. However, with the advancement of technologies, the security risk of these systems is increasing daily. Due to the presence of numerous patient records and financial data, cybercriminals consistently attempt to breach the system. In addition to sensitive data, many IoT devices can be controlled by cyber attackers, which poses a greater danger to patients, such as Braun's infusion pump or Medtronic insulin pump, simulated attacks directed at pacemakers and implantable cardiac defibrillators. These incidents occur due to the vulnerability and security failures of the systems. Additionally, insider attackers often become involved in data breaches, which compromise the sensitive health data of patients. Recent advancements, such as the HNMblock model, leverage blockchain's decentralized architecture to address healthcare system vulnerabilities. By ensuring tamper-proof data integrity, automating security protocols through smart contracts, and enabling real-time threat monitoring, this approach enhances the security and resilience of interconnected medical systems against cyber threats. Such models provide a foundation for aligning the proposed framework with existing solutions in the field, ensuring its relevance and addressing critical needs [1].

Healthcare's cybersecurity environment is alarmingly highlighted by the recent record of data breaches in this sector. A combined population of 249.09 million individuals have been impacted through healthcare data breaches throughout 2005 and 2019, demonstrating the extensive vulnerabilities in these platforms. These cases are growing increasingly severe and prevalent, as evidenced by the observation that 157.40 million people were affected in the past five years of the period [2].

The extent of these issues became more apparent in 2018 as 2,216 data breaches came to light in 65 countries, with the healthcare industry encompassing the largest proportion of these breaches (536 breaches) [3]. In the healthcare industry alone, 505 breaches resulted in the exposure, fraud, or unauthorized release of 41.2 million medical records in 2019 and there were 2,013 breaches documented worldwide from 86 nations [4]. These trends demonstrate how cybercriminals targeted the healthcare industry significantly due to its substantial amount of sensitive financial and health data with its high value.

The financial repercussions of healthcare data breaches remain equally concerning. The healthcare industry reported a significantly higher average cost of $6.45 million per breach during 2019, while the average cost of a data breach across all industries in 2019 remained $3.92 million, according to an IBM study [5]. Particularly alarming were the figures within the United States. In comparison to global standards, the average cost of a healthcare data breach within the United States increased to $15 million, with a median breach size of 25,575 records [6]. Although the cost per breached record increased by 3.4% between 2014 and 2019, the average cost of a data breach rose by 12% over the same period. Notably, the cost per compromised record increased by 19.4% in the healthcare industry, which was the highest rate of growth across all business sectors [6–9]. The healthcare industry experienced a significant increase in data breaches during the period from 2020 to 2024, compromising millions of patient records worldwide. Notable incidents include the Indonesian health agency's 2021 release of 279 million records and the Kaiser Permanente breach that affected 13.4 million users in 2024. Improperly configured cloud systems, inadequate data encryption, and the exploitation of zero-day vulnerabilities have emerged as prevalent causes. The substantial value of sensitive patient information in illicit markets renders the healthcare sector a potential target [10].

The aforementioned data demonstrate serious vulnerabilities in the healthcare sector. Given the industry's reliance on interconnected electronic systems and the sensitivity of patient data, it presents a lucrative target for cybercriminals. Beyond financial consequences, patient safety and institutional reputation are particularly at risk from healthcare cybersecurity incidents. In contrast to breaches in other business sectors, compromised health information can result in inaccurate diagnoses, inappropriate interventions, and other potentially fatal consequences. To safeguard patient health and other critical data, it has become imperative that robust cybersecurity measures be implemented expeditiously.

Connected technologies are becoming more and more important for healthcare organizations to simplify processes, improve patient care, and raise outcomes. This reliance, however, reveals important weaknesses as shown in earlier research where inadequate computing resources, unsafe setups, and different device types aggravate security issues [11]. Healthcare systems run risks compromising sensitive patient data and system functionality, much as security problems seen in IoMT systems like unprotected network ports and hard-coded passwords. Dealing with these problems calls for using cutting-edge methods to properly find and reduce hazards. Inspired by this idea, our work presents a machine learning-based framework to dynamically adjust to changing hazards, identify vulnerabilities, and prioritize them by degree of severity and probability of exploitation. This method guarantees proactive cybersecurity policies, protecting patient information, therefore strengthening the resilience of healthcare systems.

For risk assessment and vulnerability analysis, machine learning has shown to be an unavoidable tool for evaluating challenging datasets and revealing patterns that would otherwise stay latent [12,13]. These methods draw attention to how well ML models might evaluate systematic vulnerabilities. Deep learning (DL) and supervised learning have been effectively used to evaluate vulnerabilities in IoT device profiling and disaster management by means of their capacity to analyze various data sources and change with the times of threat. For example, whereas transudative transfer learning helps to profile IoT devices across diverse contexts, ML techniques such as Support Vector Machines (SVM) and Random Forests (RF) have been utilized to detect risk-prone locations in catastrophe scenarios [12,13] These methods show how well ML models might evaluate vulnerabilities methodically, hence supporting proactive decision-making. Inspired by these developments, this work creates a machine learning-based framework specifically for healthcare cybersecurity, emphasizing vulnerability identification and prioritizing to protect patient data and essential systems from developing hazards.

Emerging as a transforming tool in cybersecurity, machine learning (ML) allows the analysis of enormous datasets to identify trends suggestive of possible risks, such malware, phishing, and network intrusions [14,15]. Important for preventive security measures, anomaly detection and supervised learning models among advanced machine learning approaches have shown efficacy in recognizing anomalous activity and automating vulnerability assessments [15]. Moreover, adaptive learning and predictive analytics let systems develop dynamically to handle fresh attack routes without human intervention [14]. These techniques provide strong protection of sensitive patient data and enhance the cybersecurity resilience of linked health systems, thereby complementing the goals of our work, which intends to bring ML-based approaches to the healthcare domain.

II. Background Study

The potential use of machine learning (ML) technologies in healthcare and medicine is immense in terms of better care and lower costs [16]. Deployment of AI-based applications is involved in almost everything from a number of startup companies like Ayasdi, Apixio, Benevolent AI, Butterfly Network, Digital Reasoning systems, Flatiron Health, H2O.ai, iCarbonX, Pathway Genomics, WellTok, AliveCor etc. Interpreting large amounts of data in order to draw patterns and conclusions by aiding doctors to distinguish between various treatment options is a modern day machine learning. The cost of healthcare keeps growing and medical appointments are complex, as machine learning technology applied to modern medicine is a solution to this ever-growing issue in the healthcare domain.

The processing volumes of data and variety of domain classification is another domain of machine learning (ML) like quantum ML [17]. Quantum machine learning (QML) and various applications of QML in healthcare are benefitting many areas via rapid development and better performance compared to other healthcare models. Application domains like cybersecurity, pattern recognition, stock markets, disease diagnosis, agriculture due to ML algorithms have already benefited a lot by achieving higher accuracy. With acceleration of quantum routines, paradigms of QML techniques (quantum-facilitated support vector machines, quantum-aided ML, and varying quantum circuits), they have accelerated the ML algorithms.

Cybersecurity is a critical concern as the integration of Internet of Medical Things (IoMT) technologies within healthcare systems has expanded the attack surface. Numerous research investigations highlight how vulnerabilities, including default passwords, unencrypted data transfers, and unprotected network connections, have been introduced by the diverse nature of IoMT devices and their disparate processing capacities [18]. Significant breaches, such as unauthorized access to patient data and device operation modification, could result from these security vulnerabilities [18]. This research elucidates how advanced machine learning methods, particularly federated learning models and unsupervised anomaly detection, may enhance IoMT security through the identification of anomalous device activities in real-time without compromising patient privacy. Healthcare providers may address the inherent limitations of conventional security solutions while providing robust protection across diverse IoMT ecosystems through the implementation of these technologies. The objective of enhanced cybersecurity in healthcare has also drawn attention to the significance of innovative approaches that combine blockchain and machine intelligence. The integration of machine learning models within blockchain's decentralized architecture facilitates improved traceability, tamper-resistant data exchange, and rapid decision-making in critical situations. As a case study, it is demonstrated how blockchain smart contract technology may facilitate automated vulnerability mitigation procedures, while machine learning algorithms may continuously scan and predict potential threats using historical data. These hybrid systems are particularly effective in addressing the challenges associated with multi-party accessibility and adherence to stringent healthcare regulations such as HIPAA and GDPR. The objectives of the present investigation, aimed at developing flexible and scalable cybersecurity frameworks for healthcare systems, align with the prospective trajectory that the combination of blockchain and machine learning delineates for future research and development.

The critical role of machine learning (ML) in bolstering cybersecurity by addressing complex vulnerabilities such as Cross-Site Scripting (XSS) and Cross-Site Request Forgery (XSRF) [19]. By means of enhanced data preprocessing, real-time anomaly detection, and predictive analytics, they showed that ML frameworks can efficiently identify minor trends suggestive of cyber dangers, therefore enabling early intervention. These techniques are especially pertinent in the healthcare industry, where maintaining patient data and guaranteeing continuous service delivery take front stage. Furthermore, ML's capacity to dynamically learn and adjust to new attack paths improves its application in controlling changing threat environments. Using ML-based vulnerability assessments to prioritize risks depending on severity and likelihood, this study applies these ideas to the healthcare field enabling more effective resource allocation and proactive defense methods. This framework seeks to solve immediate and long-term cybersecurity issues in healthcare systems by leveraging the scalability and adaptability of ML approaches.

The transformative potential of machine learning (ML) in the healthcare domain, emphasizing its role in enhancing clinical decision-making and operational efficiency [20]. From real-time data analysis to customizing treatment recommendations by combining patient history, lifestyle, and genetic information, their research investigated the several uses of machine learning. Epidemic outbreak prediction was among them. Moreover, ML technologies have proven quite helpful in lowering human mistakes and improving healthcare operations including patient record management and simplification of medical imaging analysis. These results complement the aims of our work, which uses ML-based risk assessments to solve cybersecurity issues, protect patient information, and guarantee the resilience of healthcare systems against developing hazards. This study intends to show how ML can be properly used to safeguard important healthcare infrastructure by extending on these discoveries.

The critical role of blockchain technologies in addressing cybersecurity challenges in healthcare systems, particularly vulnerabilities arising from interconnected and outdated infrastructures [1]. The study underlined the need of using scalable and flexible models to guarantee real-time protection of private patient information. Healthcare companies may improve operational resilience and protect against developing threats by spotting and reducing security risks using data-driven technologies with the help of blockchain integration resulting in better machine learning implications for decision making. These results fit the objectives of this work, which investigates the use of machine learning for vulnerability assessment in order to guarantee the dependability of healthcare systems and so reinforce cybersecurity policies.

doi:10.20944/preprints202502.2165.v1

Table 1. Opportunities & challenges of using machine learning based vulnerability assessment in Health Systems.

Aspect	Opportunities	Challenges	Ref
Enhancing Clinical Decision-Making	Improves treatment recommendations and epidemic outbreak predictions through real-time data analysis.	Integrating diverse data sources such as patient history and genetic information.	[20]
Addressing Complex Cybersecurity Threats	Enables early detection and mitigation of vulnerabilities such as XSS and XSRF through dynamic ML models.	Constantly updating models to address evolving threats and ensure data security.	[19]
Optimizing Healthcare Operations	Reduces human errors and streamlines medical imaging and patient record management.	Managing noisy data and maintaining operational efficiency at scale.	[20]
Quantum Machine Learning Applications	Accelerates algorithms for disease diagnosis and medical imaging through quantum routines	Limited quantum infrastructure and complexity in translating medical data to quantum states.	[17]
Reducing Costs in Healthcare	Leverages ML technologies to interpret large datasets, aiding in distinguishing treatment options while reducing costs.	Balancing the cost of implementing ML technologies with achieving measurable outcomes.	[16]
Addressing Vulnerabilities in Interconnected Infrastructures	Proposes a scalable and adaptable blockchain model to enhance real-time protection of sensitive patient information and improve vulnerability assessments, yielding better outcomes through the integration of machine learning.	Requires continuous monitoring and adaptation to mitigate risks in outdated and interconnected infrastructures.	[1]

III. Emerging Threats in Healthcare Domain

As several types of cyber threats are going on and the healthcare domain is being the most attacked critical infrastructure, another frequent attack is the internal threats [21]. Data breaches are now part of healthcare critical infrastructure and there is no complete solution to counter the insider attacks. Several ransomware attacks (like WannaCry ransomware) have halted business and finance firms for days, weeks, and months including the need for patient centered policy and user education. Multiple security measures should be used together (instead of single measure) as the US Department of Health and Human Resources identified data disclosure incidents as major ones.

Patient wearable devices and other entities share accumulated data and follow unstructured communication which is another primary challenge and threat for healthcare internet of things (IoT) [22]. Security challenges for healthcare stakeholders due to open-area deployment as IoT applications are switching from different domains including logistics, smart cities, healthcare, and many more. Sending data from source node to destination node is exposed to operational environment threats and attackers can easily take advantage (say, base station attacks, DDoS attacks) of that.

Advanced technologies, including Wireless Body Area Networks (WBANs), which allow real-time monitoring and patient data transmission for better healthcare outcomes, have been adopted in the healthcare arena with great surge. These systems bring major flaws even if they have advantages. WBAN devices are easy targets for cyberattacks since they can run with little computational resources, which limits their capacity to apply sophisticated security mechanisms. Attackers directly compromise patient safety by using these constraints to execute data manipulation, denial-of- service (DoS) assaults, or even intercept and change medical information [23]. Furthermore, the linked character of these systems means that a compromise in one device might spread over the network and cause cascading failures in important healthcare activities. The absence of strong cryptographic systems and ongoing authentication presents a significant obstacle since sensitive information is left open to usage and interception. Third-party software and gadgets, which might not have enough security control, accentuate these flaws. Implementing adaptive security systems that use cutting-edge technologies like machine learning to identify anomalies, forecast possible attack paths, and therefore reduce risks proactively would help to counter these developing hazards. Maintaining confidence and safety in healthcare systems depends on patient data being confidentially, ethically available in these changing technological environments.

Driven by the fast digitization and interconnectedness of medical infrastructures, healthcare institutions now deal with an increasing range of cyber challenges. Healthcare companies are more vulnerable as sensitive assets including electronic health records (EHRs), medical devices, and research data become main targets. Attackers launch ransomware assaults, data breaches, and even system-wide outages using underfunded IT infrastructure, legacy system weaknesses, and poor security standards. With an estimated $50 per record, the great value of patient records on the illicit market motivates enemies ranging from small-time hackers to nation-state players [24]. Emerging risks such targeted ransomware, which paralyzes vital healthcare activities, and untargeted attacks using weak holes in linked systems have underlined how urgently adaptive security measures are needed. These difficulties call for strong systems that combine advanced analytics with real-time monitoring to provide resilience against both known and changing hazards.

Although the digital revolution of healthcare systems greatly enhances operational efficiency and patient outcomes, it also brings a complicated terrain of cybersecurity issues. Because of their high-value data and operational relevance, critical infrastructures including electronic health records (EHRs), Internet of Medical Things (IoMT), and linked devices top priorities. Emerging risks include vulnerabilities in outdated systems that fall short of contemporary security criteria, insider threats resulting from illegal access or carelessness, and ransomware assaults upsetting important medical services [25]. Furthermore, aggravating the concerns are the spread of bring-your-own-device (BYOD) rules, unencrypted storage of critical data, and dependence on unprotected networks. Targeting human, corporate, and technological levels of the system, advanced persistent threats (APTs) and multi-layered attacks further complicate the problem. Dealing with these issues calls for a complete cybersecurity strategy including proactive mitigating techniques, dynamic risk assessment models, and threat intelligence to guarantee the confidentiality, integrity, and availability of important healthcare data.

Table 2. Emerging threats and cyberattacks with their threat types in the healthcare domain (healthcare systems) along with several insights provided.

Ref.	Threat type	Threat Insight 1	Threat Insight 2
[21]	Internal Threats - Healthcare Critical Infrastructure	Attack on the UK National Health Service wannaCry ransomware.	Major theoretical shortfall in current cyber defense architecture.

[22]	Security Threats - Healthcare Internet of Things	Open-area deployment & wireless communication security challenge.	Accumulated data sharing and unstructured communication
[23]	Security Threats - Wireless Body Area Networks (WBANs)	WBAN devices with limited computational resources are prone to cyberattacks, including data manipulation, denial-of-service (DoS) attacks, and medical information interception.	The absence of robust cryptographic protections and continuous authentication, coupled with the cascading impact of device compromises across networks, threatens critical healthcare operations.
[24]	Security Threats - Healthcare Cybersecurity Challenges	The high value of patient records ($50 per record) on the illicit market makes healthcare institutions prime targets for ransomware attacks, data breaches, and system outages. Attackers range from small-time hackers to nation-state actors, motivated by financial gain.	Weaknesses in legacy systems, underfunded IT infrastructure, and poor security practices create vulnerabilities in healthcare systems, exposing them to both targeted ransomware and untargeted attacks exploiting interconnected system flaws.
[25]	Internal Threats - Electronic Health Records, IoMT, & BYOD	Critical infrastructures such as electronic health records (EHRs), Internet of Medical Things (IoMT), and connected devices are prime targets for cyberattacks due to their high-value data and operational importance. Emerging risks include vulnerabilities in outdated systems, insider threats, and ransomware attacks disrupting critical medical services.	The proliferation of bring-your-own-device (BYOD) policies, unencrypted storage of sensitive data, and reliance on unsecured networks amplify the risk, making healthcare systems more vulnerable to advanced persistent threats (APTs) and multi-layered attacks targeting human, organizational, and technical layers of security.

IV. Vulnerability Assessment via ML

Vulnerability assessment plays a critical role in identifying, evaluating, and addressing weaknesses in systems and networks. With the rapid escalation in cyber threats and the complexity of modern infrastructures, machine learning (ML) has emerged as a transformative tool for enhancing these assessments. By automating the detection process, analyzing vast datasets, and predicting vulnerabilities, ML methods address the limitations of manual and static rule-based approaches, providing a scalable and adaptive solution [26].

ML models enable efficient identification of vulnerabilities by analyzing patterns and anomalies in system behaviors, Supervised learning algorithms, such as Support Vector Machines and Random Forests, rely on historical data to classify system states as secure or vulnerable. These methods excel at detecting known vulnerabilities by learning from labeled datasets. However, undocumented vulnerabilities require unsupervised learning approaches, such as clustering algorithms and autoencoders, which identify deviations from normal system behavior. For instance, anomalies in network traffic could signify a security breach [27].

Reinforcement learning further enhances ML's adaptability in dynamic environments by continuously improving its detection capabilities through iterative feedback and system interactions. This is particularly valuable for real-time vulnerability detection and remediation in environments with rapidly evolving threats [28]. Natural Language Processing (NLP) is also gaining traction in this domain, analyzing unstructured data like system logs and threat intelligence reports to extract actionable insights, thereby improving both vulnerability detection and prioritization [29].

A significant advantage of ML-based vulnerability assessment lies in its predictive capabilities. By leveraging historical trends and current threat intelligence, predictive models can forecast potential vulnerabilities before exploitation, enabling proactive countermeasures [30]. These capabilities are particularly crucial in complex and sensitive environments such as healthcare systems, where interconnected devices and patient data demand robust security measures.

Despite its potential, ML-driven vulnerability assessment faces challenges. High-quality datasets are essential for training ML models, but acquiring and labeling such data can be resource-intensive. Additionally, adversarial attacks, where attackers manipulate data to mislead ML models, pose a significant risk. The computational expense of training advanced ML algorithms can also be a barrier, particularly for organizations with limited resources.

Hybrid approaches that incorporate multiple machine learning methods are becoming increasingly prevalent in an effort to enhance the efficacy of ML-driven vulnerability assessment. For instance, comprehensive coverage may be achieved by combining unsupervised learning to detect unexpected anomalies with supervised instruction on recognizing established threats. Similarly, the ensemble learning method improves effectiveness and reduces the likelihood of false positives by aggregating the predicted outcomes of multiple models. Recent advancements in federated learning, which trains models on distributed endpoints without transmitting raw data, address privacy concerns and ensure compliance with regulatory requirements such as GDPR and HIPAA. These techniques are particularly significant in sensitive domains like healthcare, where protecting patient information is crucial. Organizations can enhance their countermeasures against complex and dynamic cyber threats while maintaining data compliance and security requirements through the implementation of such hybrid approaches.

V. Patient Data, Patient Safety, and Cyber-attacks

Data breaches are increasing every year because cyberattacks on the healthcare system are increasing ever more than before. The illegal use of PII (personal identifiable information) on data breach cyberattacks and several implantable medical devices with dangers of wireless connections cyberattacks [31,32]. More generally throughout medicine, risk of many patients suffering harm due to cybersecurity failures in modern implantable medical devices (IMD). The key recommended solutions in terms of security of medical devices are auditing (detailed logs of device activity and events), bug reporting (identifying security flaws and patching them), multi-factor authentication (MFA, more challenge for attackers), and education (awareness of cybersecurity risk among clinicians).

Cyberattacks using Internet of Things (IoT) as the rise of digital technology with several new algorithms proposed for patient data security and network security for healthcare systems [33]. Since the outbreak of COVID-19, hackers are applying several covid-based schemes (primarily targeted for patients) for cyberattacks in healthcare domains. Challenges highlighting the need for patient data security and effective data maintenance are urgent at nations (developed countries) such as the United Kingdom, United States, India, Russia etc. Healthcare systems witnessed malware attacks, database hacks, password attacks and data phishing, unauthorized access to patient data, apart from disruption of telemedicine and virtual treatment services (some major data breaches in Table 3 for patient data). The major algorithms applied to healthcare systems (DES, AES, 3DES, RSA, and many more) are attacked by hackers using several techniques like Hashing, Salting, and Brute-Force Attacks.

Table 3. Biggest data breaches and hacks for patient data and healthcare system.

(Source: Information is beautiful visualizations of biggest data breaches and hacks [34])

SN	Data Breaches	Cyberattacks on Patient data and healthcare	Year
1.	Dutch government data lost	Loses hard drive with data of 6.9 million registered donors, from Dutch Minister of Health, Wellness	2020
2.	Cense AI medical data leak	Artificial Intelligence company, Cense AI leaks over 2.5 million medical records, publicly visible on the internet	2020
2.	Indonesia's health agency	Personal information of 279 million Indonesians (data stored by BPJS Kesehatan, country's healthcare and social security agency)	2021
3.	Contact tracing Info	Exposed data was all stored in Microsoft's PowerApps portal service, 38 million records on open internet	2021
4.	FlexBooker appointing scheduling breach	Over 3.7 million accounts impacted, US-based appointment scheduling service stolen in cyberattack	2022
5.	Maximus zero-day flaw	US government service contractor, having sponsored-programs, federal & local healthcare programs, disclosed data breach of 8 - 11 million people	2023
6.	Sav-Rx prescription data breach	Prescription management company, Sav-Rx, impacting 2.8 million Americans, personal data was stolen	2023
7.	Welltok data breach	8.5 million US patients, Healthcare SaaS provider Welltok, file transfer was hacked in data theft attack	2023
8.	TIAA data breach	Financial organization, TIAA provides retirement plans, life insurance, 2.3 million individuals, exposed personal information via unauthorized party access	2023
9.	Kaiser Permanente data transmitted	Leading healthcare organization in US, Kaiser Permanente, disclosed data breach impacting 13.4 million of its patients and members	2024

doi:10.20944/preprints202502.2165.v1

VI. Proposed Framework – healthMLsec

The healthMLsec framework is a machine learning-based system designed to enhance cybersecurity and protect patient data within healthcare organizations. This framework aims to identify and mitigate vulnerabilities by leveraging machine learning algorithms to analyze system and network data, detect potential threats, and prioritize vulnerabilities based on their severity. The framework's core components are outlined below:

6.1. Data Collection and Preprocessing

The first step of the healthMLsec framework involves gathering extensive data from healthcare systems, including network logs, system configurations, and historical attack patterns. The data is then preprocessed to ensure consistency and suitability for machine learning models. Key preprocessing steps include:

- *Data Normalization:* It ensures uniformity across diverse data sources [35].
- *Data Cleansing*: It removes irrelevant or erroneous data, enhancing model accuracy [36].
- *Feature Extraction*: It identifies relevant patterns, such as anomalous traffic or unauthorized access attempts.

6.2. Vulnerability Detection Using Machine Learning

At the heart of the healthMLsec framework is its use of machine learning techniques to detect vulnerabilities in real-time. These techniques analyze system and network data to identify patterns indicative of potential security weaknesses. Various machine learning models are used, including:

- *Supervised Learning Models:* These models, such as Random Forests, Support Vector Machines (SVM), and Neural Networks, are trained on historical attack data to identify known attack signatures and vulnerabilities [37].
- *Unsupervised Learning Models:* Clustering algorithms like K-means or anomaly detection methods are employed to discover novel vulnerabilities that may not have been previously documented [19].
- *Reinforcement Learning:* In dynamic environments, reinforcement learning can adapt and improve vulnerability detection by learning from new data and constantly evolving threats [38].

The use of these algorithms enables the framework to continuously adapt to emerging cybersecurity threats and improve its detection capabilities.

6.3. Prioritization of Vulnerabilities

After identifying potential vulnerabilities, the next critical step is to prioritize them based on their risk level and likelihood of exploitation. The healthMLsec framework uses a risk-based approach to ensure that resources are directed toward the most critical issues. This prioritization is achieved by considering:

- *Exploitability Score:* How likely a vulnerability is to be exploited based on historical data and current system configuration [39].
- *Impact Assessment:* Evaluating the potential consequences of a vulnerability being exploited, such as data breaches, system downtime, or patient safety risks [40].
- *Threat Intelligence:* Integrating up-to-date threat intelligence feeds to assess the current threat landscape and adjust vulnerability priorities accordingly [41].

The framework generates a Vulnerability Risk Score (VRS) for each identified vulnerability, which is then used to allocate resources for remediation efforts.

6.4. Remediation and Mitigation Strategy

Once vulnerabilities are prioritized, the framework suggests actionable remediation strategies. These include:

- *Patch Management:* Ensuring security patches and updates are applied to vulnerable systems promptly.
- *System Hardening:* Modifying system configurations to reduce the attack surface, such as disabling unnecessary services or closing unused ports.
- *Access Control Policies:* Strengthening access control and authentication mechanisms to limit unauthorized access to critical systems [42].
- *Incident Response Plan:* If a breach or attack is detected, the framework guides the development of an incident response plan to mitigate the damage and prevent future occurrences.

The proposed mitigation strategies are tailored to the healthcare environment, ensuring that patient safety is not compromised during the implementation of security measures.

6.5. Continuous Learning and Adaptation

One of the key advantages of healthMLsec is its ability to learn and adapt over time. As new vulnerabilities are discovered and new attack techniques emerge, the framework continuously updates its models by incorporating new data. This allows healthcare organizations to maintain an effective defense against evolving cyber threats. The adaptation process includes:

- *Model Retraining:* Periodically retraining the machine learning models with new attack data to improve accuracy and relevance [43].
- *Feedback Loop:* Integrating feedback from security incidents and remediation actions into the system to enhance its predictive capabilities.

This continuous learning process ensures that healthMLsec remains effective even as cyber threats evolve.

6.6. Compliance and Regulatory Standards

The healthMLsec framework is designed to help healthcare organizations meet industry regulations and standards for cybersecurity and patient data protection, such as HIPAA, GDPR, and other national or international healthcare security frameworks. By integrating compliance checks into the vulnerability assessment process, the framework ensures that all identified vulnerabilities are also evaluated for their impact on regulatory compliance. This integration helps healthcare organizations maintain patient trust and avoid potential legal liabilities.

6.7. Visualization and Reporting

Visualization and Reporting is a user-friendly dashboard that provides healthcare administrators with a clear, actionable view of their system’s security status. The dashboard includes:

- *Vulnerability Overview:* A summary of detected vulnerabilities, their risk levels, and their current remediation status.
- *Risk Heat Map:* A visual representation of the system’s security landscape, highlighting areas of high vulnerability.
- *Audit Trail:* A record of all remediation actions taken, ensuring traceability and accountability.
- *Compliance Status:* A summary of how well the organization is meeting regulatory requirements.

This visualization empowers healthcare organizations to make informed decisions and quickly respond to emerging security threats.

6.8. User Feedback and Security Governance

The framework emphasizes adaptability and compliance through:

- *User Feedback:* Collected via surveys and secure reporting portals, it refines ML models and addresses usability challenges.
- *Security Governance:* Establishes policies, roles, and mechanisms to monitor threats, conduct audits and mitigate risks [44].

Together, these components create a feedback loop that optimizes system performance and reinforces trust in healthcare cybersecurity. The healthMLsec framework represents a comprehensive and proactive approach to cybersecurity in healthcare systems. By integrating machine learning techniques with vulnerability management and continuous adaptation, it enables healthcare organizations to identify, assess, and mitigate risks in real time. This approach not only enhances the protection of patient data but also strengthens the overall security posture of healthcare organizations, helping them comply with regulatory standards and respond effectively to emerging threats.

VII. Conclusion

In healthcare, the advent of technology has undoubtedly improved patient outcomes, connectivity, and efficiency. However, this has also introduced an increasing array of cybersecurity challenges that compromise healthcare data, disrupt operations, and undermine organizational trust. This paper proposes the healthMLsec framework, a machine learning-based approach that automates vulnerability identification, prioritization, and mitigation to address these issues. The system utilizes reinforcement, unsupervised, and supervised learning approaches for identifying both known and unknown threats, enabling hospitals and clinics to implement rapid, evidence-based solutions. Organizations can also anticipate vulnerabilities based on its predictive features, resulting in a proactive approach to cybersecurity.

One of the primary strengths of the healthMLsec framework is its adaptability to the specific requirements of healthcare organizations. It ensures that security protocols are both effective and appropriate by employing sophisticated risk-management techniques, incorporating real-time threat intelligence, and adhering to regulatory frameworks such as HIPAA and GDPR. Through its mechanisms for continuous learning, the framework can adapt to emerging threats and enhance the resilience of healthcare systems. The proposed architecture provides a robust foundation for developing reliable, flexible, and effective security measures tailored to healthcare needs, despite challenges such as data quality standards, computational overhead, and the potential for adversarial attacks.

The healthMLsec framework presents significant potential for advancements in healthcare cybersecurity in the near future. While addressing ethical considerations such as fairness and transparency in AI-driven security frameworks could enhance its acceptability, integrating emerging technologies like blockchain and quantum machine learning could further expand its capabilities. In addition to safeguarding patient data, healthMLsec fosters trust in electronic healthcare systems by emphasizing a comprehensive and proactive strategy. By ensuring secure, reliable, and sustainable systems that are prepared to address current and future challenges, this research advances the field of cybersecurity in the healthcare sector.

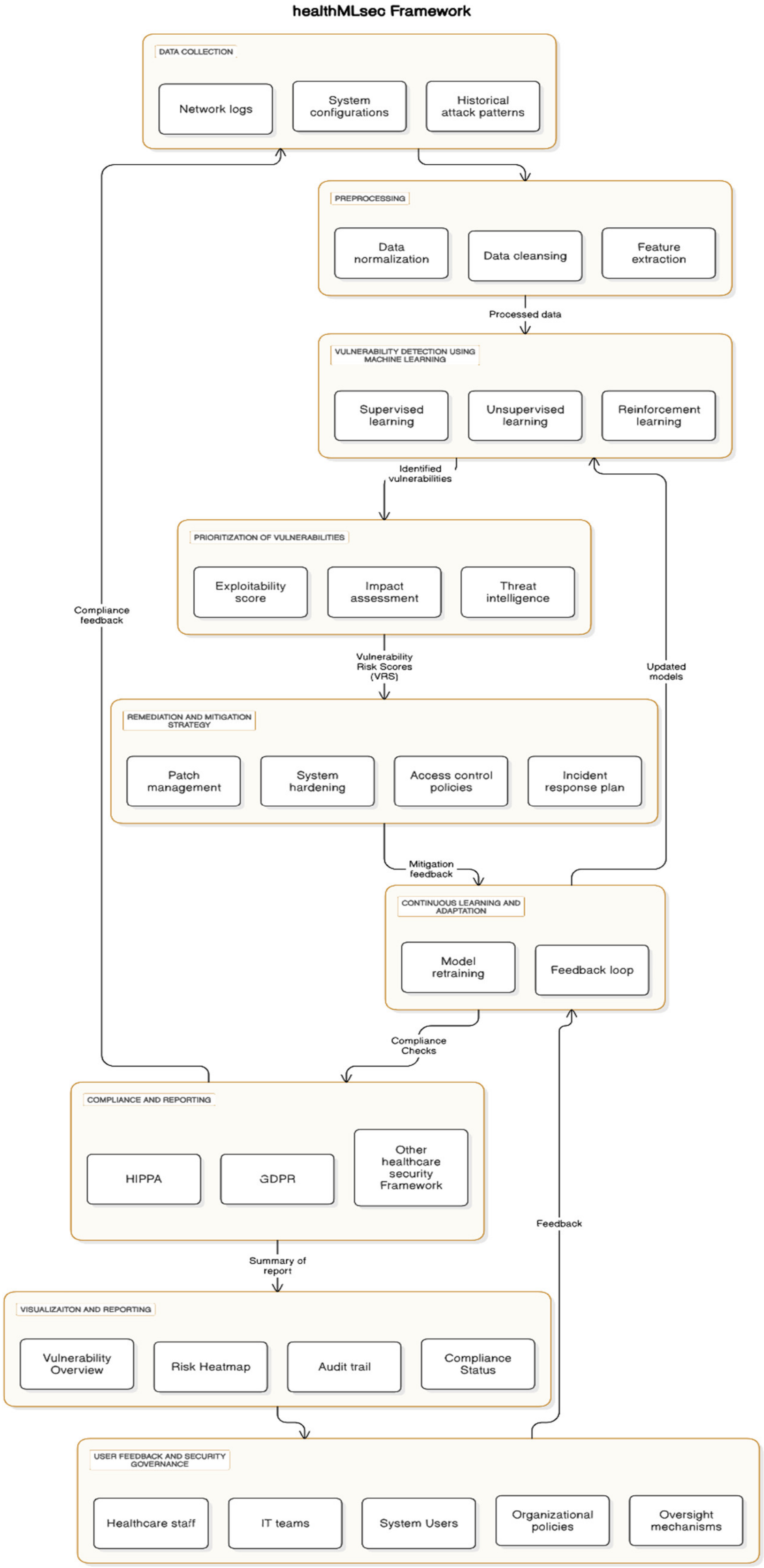

Figure 1. healthMLsec Framework (proposed).

References

1. Kshetri, N., Mishra, R., Rahman, M. M., & Steigner, T. (2024). *HNMblock: Blockchain Technology Powered Healthcare Network Model for Epidemiological Monitoring, Medical Systems Security, and Wellness.* In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 01–08). IEEE. https://doi.org/10.1109/ISDFS60797.2024.10527226
2. Privacy Rights Clearinghouse. "Data Breaches | Privacy Rights Clearinghouse." Privacy Rights.org, 2020, privacyrights.org/data-breaches
3. Verizon. (2018). 2018 Data Breach Investigations Report. Verizon Enterprise Solutions. https://www.verizon.com/business/resources/reports/DBIR_2018_Report.pdf
4. Alder, Steve. "December 2019 Healthcare Data Breach Report." HIPAA Journal, 21 Jan. 2020, www.hipaajournal.com/december-2019-healthcare-data-breach-report/.
5. IBM. (2020). How much would a data breach cost your business? Retrieved January 12, 2020, from https://www.ibm.com/security/data-breach
6. HIPAA Journal. (2020). 2019 cost of a data breach study reveals increase in U.S. healthcare data breach costs. Retrieved February 15, 2020, from https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/
7. Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. Perspectives in Health Information Management, 11, 1–16.
8. Ponemon Institute. (2015). 2015 cost of data breach study: Global analysis. Retrieved February 28, 2020, from https://www.ponemon.org/local/upload/file/2015%20Global%20CODB%20FINAL%203%20copy.pdf
9. IBM. (2019). 2019 cost of a data breach report. Retrieved February 17, 2020, from https://www.ibm.com/downloads/cas/ZBZLY7KL
10. Verizon. "2024 Data Breach Investigations Report." Verizon Business, 2024, www.verizon.com/business/resources/reports/dbir/
11. Rajawat, A. S., Goyal, S. B., Bedi, P., Jan, T., Whaiduzzaman, M., & Prasad, M. (2023). Quantum machine learning for security assessment in the Internet of Medical Things (IoMT). *Future Internet*, *15*(8), 271.
12. Linardos, V., Drakaki, M., Tzionas, P., & Karnavas, Y. L. (2022). Machine learning in disaster management: recent developments in methods and applications. *Machine Learning and Knowledge Extraction*, *4*(2).
13. Danso, P. K., Dadkhah, S., Neto, E. C. P., Zohourian, A., Molyneaux, H., Lu, R., & Ghorbani, A. A. (2023). Transferability of machine learning algorithm for IoT device profiling and identification. *IEEE Internet of Things Journal*.
14. Balantrapu, S. S. (2023). Future Trends in AI and Machine Learning for Cybersecurity. *International Journal of Creative Research In Computer Technology and Design*, *5*(5).
15. Ozkan-Ozay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*.
16. Bhardwaj, R., Nambiar, A. R., & Dutta, D. (2017, July). A study of machine learning in healthcare. In *2017 IEEE 41st annual computer software and applications conference (COMPSAC)* (Vol. 2, pp. 236-241). IEEE.
17. Rani, S., Pareek, P. K., Kaur, J., Chauhan, M., & Bhambri, P. (2023, February). Quantum machine learning in healthcare: Developments and challenges. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-7). IEEE.
18. Rani, Sita, et al. "Federated Learning for Secure IoMT-Applications in Smart Healthcare Systems: A Comprehensive Review." Knowledge-Based Systems, 22 May 2023, p. 110658, www.sciencedirect.com/science/article/pii/S0950705123004082, https://doi.org/10.1016/j.knosys.2023.110658.
19. Kshetri, N., Kumar, D., Hutson, J., Kaur, N., & Osama, O. F. (2024, April). algoXSSF: Detection and analysis of cross-site request forgery (XSRF) and cross-site scripting (XSS) attacks via Machine learning algorithms. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-8). IEEE.
20. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Rab, S. (2022). Significance of machine learning in healthcare: Features, pillars, and applications. *International Journal of Intelligent Networks*, *3*, 58-73.

21. Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access*, *6*, 25167-25177.
22. Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare internet of things: Security threats, challenges, and future research directions. *IEEE Internet of Things Journal*.
23. Mucchi, L., Jayousi, S., Martinelli, A., Caputo, S., & Marcocci, P. (2019, May). An overview of security threats, solutions, and challenges in wbans for healthcare. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (pp. 1-6). IEEE.
24. Le Bris, A., & El Asri, W. (2016). State of cybersecurity & cyber threats in healthcare organizations. *ESSEC Business School*, *12*.
25. Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., ... & Magalini, S. (2020, July). Cyber-attacks and threats for healthcare–a multi-layer thread analysis. In *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)* (pp. 5705-5708). IEEE.
26. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys &amp; Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/comst.2015.2494502
27. Kumar Singh, Dr. S., Vadi, Dr. V. R., Usmani, Dr. A., & Nayak, Dr. P. (2024). Algorithms of machine learning for cloud computing security. *IMRJR*, *1*(1). https://doi.org/10.17148/imrjr.2024.010106
28. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/sp.2010.25
29. Shah, I. A., Jhanjhi, N. Z., & Brohi, S. N. (2024). Machine learning models for detecting software vulnerabilities. *Advances in Web Technologies and Engineering*, 1–40.
30. Thawait, N. K. (2024). Machine learning in cybersecurity: Applications, challenges, and Future Directions. *International Journal of Scientific Research in Computer Science, Engineering, and Information Technology*, *10*(3), 16–27. https://doi.org/10.32628/cseit24102125
31. Meisner, M. (2017). Financial consequences of cyber-attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63-73.
32. Pycroft, L., & Aziz, T. Z. (2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices*, *15*(6), 403-406.
33. Kavitha, A., Rao, B. S., Akthar, N., Rafi, S. M., Singh, P., Das, S., & Manikandan, G. (2022). A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT. *International Journal of Electrical and Electronics Research (IJEER)*, *10*(2), 270-275.
34. Information is Beautiful, World's Biggest Data Breaches & Hacks, Selected events over 30,000 records stole, https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
35. Bhardwaj, R., Nambiar, A. R., & Dutta, D. (2017). A study of machine learning in Healthcare. 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), 236–241. https://doi.org/10.1109/compsac.2017.164
36. Rani, S., Kumar Pareek, P., Kaur, J., Chauhan, M., & Bhambri, P. (2023). Quantum machine learning in Healthcare: Developments and challenges. *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 1–7. https://doi.org/10.1109/icicacs57338.2023.10100075
37. Linardos, V., Drakaki, M., Tzionas, P., & Karnavas, Y. (2022). Machine learning in disaster management: Recent developments in methods and applications. *Machine Learning and Knowledge Extraction*, *4*(2), 446–473. https://doi.org/10.3390/make4020020
38. Rajawat, A. S., Goyal, S. B., Bedi, P., Jan, T., Whaiduzzaman, M., & Prasad, M. (2023). Quantum Machine Learning for Security Assessment in the internet of medical things (IOMT). *Future Internet*, *15*(8), 271. https://doi.org/10.3390/fi15080271
39. Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. *IEEE Access*, *6*, 25167–25177. https://doi.org/10.1109/access.2018.2817560

40. Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare internet of things: Security threats, challenges, and future research directions. *IEEE Internet of Things Journal*, *11*(11), 19046–19069. https://doi.org/10.1109/jiot.2024.3360289
41. Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., Tanasache, F. D., Palleschi, A., Ciccotelli, C., Sakkalis, V., & Magalini, S. (2020). Cyber-attacks and threats for healthcare – a multi-layer thread analysis. *2020 42nd Annual International Conference of the IEEE Engineering in Medicine &amp; Biology Society (EMBC)*, 5705–5708. https://doi.org/10.1109/embc44109.2020.9176698
42. Javaid, M., Haleem, A., Pratap Singh, R., Suman, R., & Rab, S. (2022). Significance of machine learning in Healthcare: Features, pillars, and applications. *International Journal of Intelligent Networks*, *3*, 58–73. https://doi.org/10.1016/j.ijin.2022.05.002
43. Danso, P. K., Dadkhah, S., Pinto Neto, E. C., Zohourian, A., Molyneaux, H., Lu, R., & Ghorbani, A. A. (2024). Transferability of machine learning algorithm for IOT device profiling and identification. *IEEE Internet of Things Journal*, *11*(2), 2322–2335. https://doi.org/10.1109/jiot.2023.3292319
44. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01161-7

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.